802.11g Wireless LAN PC Card

User Manual

Version: 1.0
(March, 2004)

COPYRIGHT

Copyright ©2004/2005 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission
Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for Certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such a PDAs or lappads is not authorized. This transmitter is restricted for use with the specific antenna(s) tested in the application for Certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 INTRODUCTION 1

1.1 Features 1

1.2 Specifications 1

1.3 Package Contents 2

2 INSTALLATION PROCEDURE 3

3 CONFIGURATION UTILITY 6

3.1 Site Survey 6

3.2 Profile 7

3.2.1 Configure the Profile 8

3.2.2 Enable WPA in Windows XP 11

3.2.3 802.1x Setting _ Evidence 11

3.2.4 802.1x Setting _ CA Server 11

3.3 Link Status 17

3.4 Statistics 18

3.5 Advance 18

3.6 About 20

4 TROUBLESHOOTING 21

1 Introduction

Thank you for purchasing the 802.11g Wireless LAN PC Card. This card complies with IEEE 802.11g standard, which supports up to 54Mbps high-speed wireless network connections. It can also work with IEEE 802.11b devices. When the card connects to 11b devices, the link speed will be up to 11Mbps.

For WLAN security issues, this card supports 64/128-bit WEP data encryption that protects your wireless network from eavesdropping. It also supports WPA (Wi-Fi Protected Access) feature that combines IEEE 802.1x and TKIP (Temporal Key Integrity Protocol) technologies. Client users are required to authorize before accessing to APs or AP Routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key. This card has built-in AES engine which ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

The power consumption of the card is also very low. Furthermore, this card provides several levels of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices.

This card is cost-effective, together with the versatile features; it is the best solution for you to build your wireless network.

1.1 Features

- Works with both IEEE 802.11b and IEEE 802.11g products.
- High-speed transfer data rate - up to 54Mbps.
- High throughput supports multi-media data bandwidth requirement.
- Supports 64/128-bit WEP, WPA (TKIP with IEEE 802.1x) and AES functions for high level of security.
- Automatic fallback increases data security and reliability.
- Supports the most popular operating system: Windows 98SE/Me/2000/XP.
- Supports 32-bit Cardbus interface.

1.2 Specifications

- Standard: IEEE 802.11b/g
- Interface: 32-bit Cardbus
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)

  BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP Data Encryption, WPA, AES and IEEE 802.1x

- Antenna: Printed Antenna with Diversity System
- Drivers: Windows 98SE/Me/2000/XP
- LEDs: TX/RX, Link
- Transmit Power: 16dBm~18dBm
- Power consumption: Tx: 350mA, Rx: 250mA
- Receive Sensitivity: 54Mbps OFDM, 10% PER, -70dBm, 11Mbps CCK, 8% PER, -86dBm, 1Mbps BPSK, 8% PER, -92dBm
- Dimension: 8(H) x 118(W) x 54(D) mm
- Temperature: 32~131 °F (0 ~55 °C)
- Humidity: Max. 95% (NonCondensing)
- Certification: FCC, CE

1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One PC Card
- One CD (Driver/Utility/User's Manual.)
- One Quick Guide

If any of the above items is missing, contact your supplier as soon as possible.

2 Installation Procedure

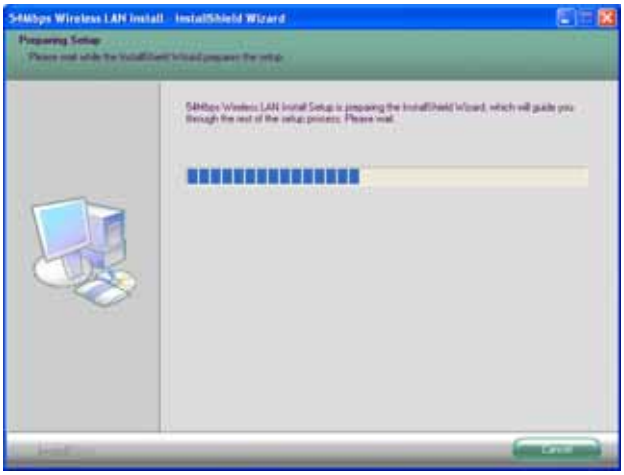
Before you proceed with the installation, please notice following descriptions.

Note1: Please do not install the card into your laptop computer before installing the software program from the CD.

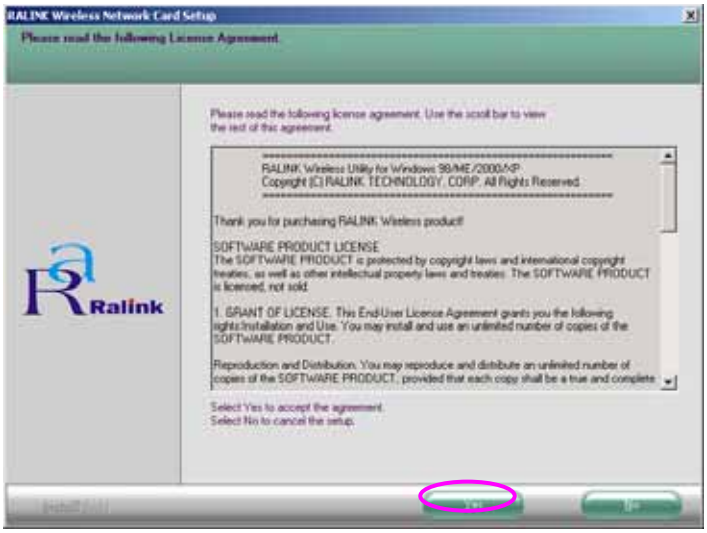
Note2: The following installation was operated under Windows XP. (Procedures are similar for Windows 98SE/Me/2000.)

Note3: If you have installed the Wireless PC Card driver & utility before, please uninstall the old version first.

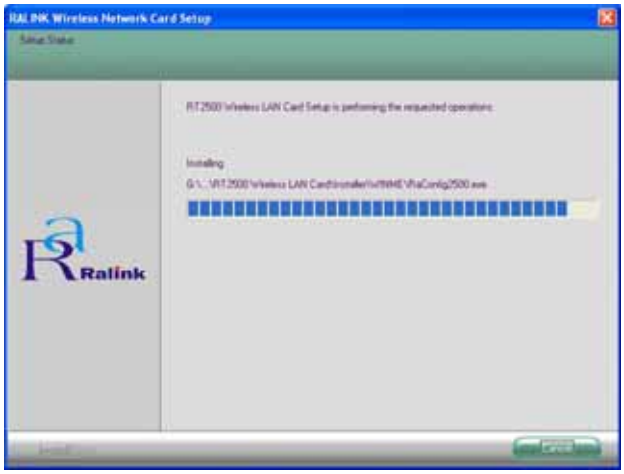
A. Insert the Installation CD to your CD-ROM Drive. Execute the “setup” program.

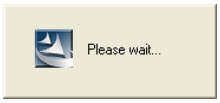


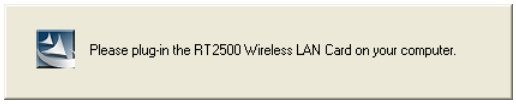
B. Click “Yes” to continue.


RALINK Wireless Network Card Setup
Please read the following License Agreement.
Please read the following license agreement. Use the scroll bar to view the rest of this agreement.
RALINK Wireless Utility for Windows 98/ME/2000/XP
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.
Thank you for purchasing RALINK Wireless product!
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete
Select Yes to accept the agreement.
Select No to cancel the setup.
Ralink

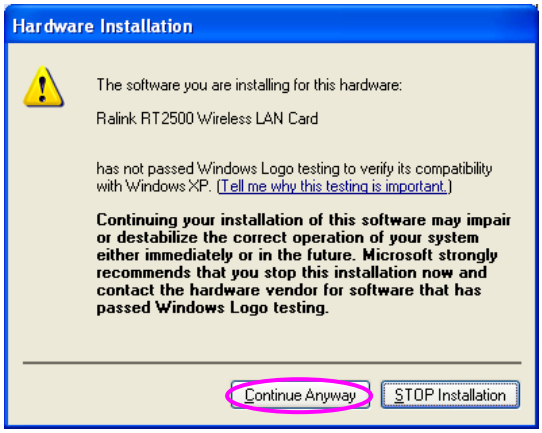
C. The system starts to install the software of the card. Follow the instruction of the program to plug in the PC card into the Cardbus slot of your laptop computer.

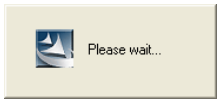




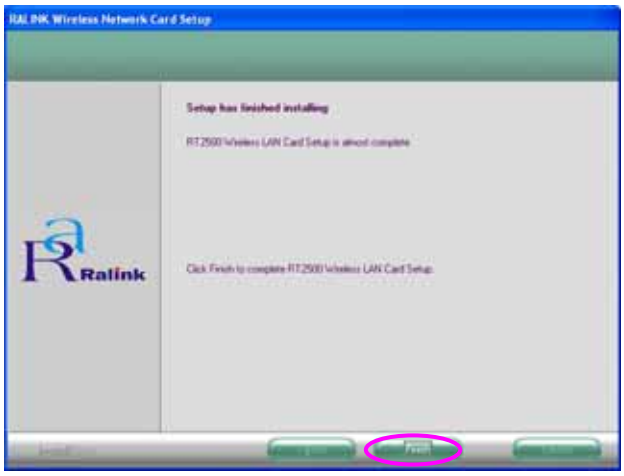


D. The system will automatically detect the card and display “Hardware Installation” screen. Click “Continue Anyway” to continue.

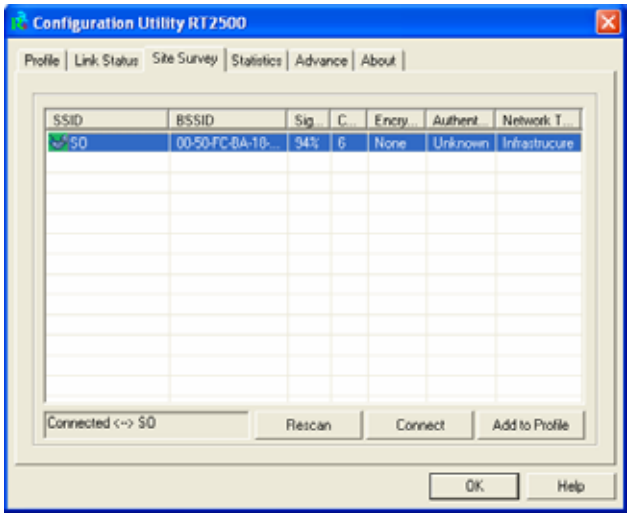

Hardware Installation
The software you are installing for this hardware:
Ralink RT2500 Wireless LAN Card
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation



E. Click “Finish” to complete the installation.


RAL INK Wireless Network Card Setup
Setup has finished installing
RT2500 Wireless LAN Card Setup is almost complete
Click Finish to complete RT2500 Wireless LAN Card Setup
Ralink
Finish

F. The “RaConfig” utility is displayed and you can start to configure the card.



3 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the PC card and monitor the link status and the statistics during the communication process.

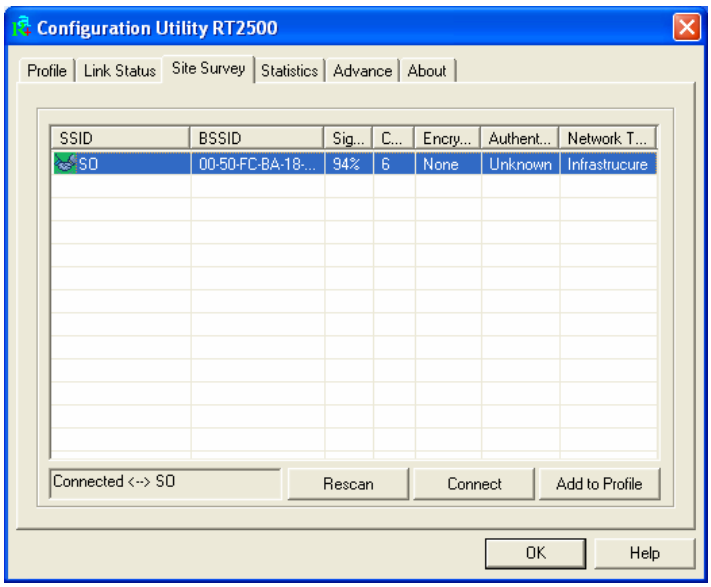
The Configuration Utility appears as an icon on the system tray of Windows while the card is running. You can open it by double-click on the icon.

Right click the icon, there are some items for you to operate the configuration utility.

- Lauch Config Utilities
  Select “Lauch Config Utilities” to open the Configuration Utility tool.
- Exit
  Select “Exit” to close the Configuration Utility tool.

3.1 Site Survey

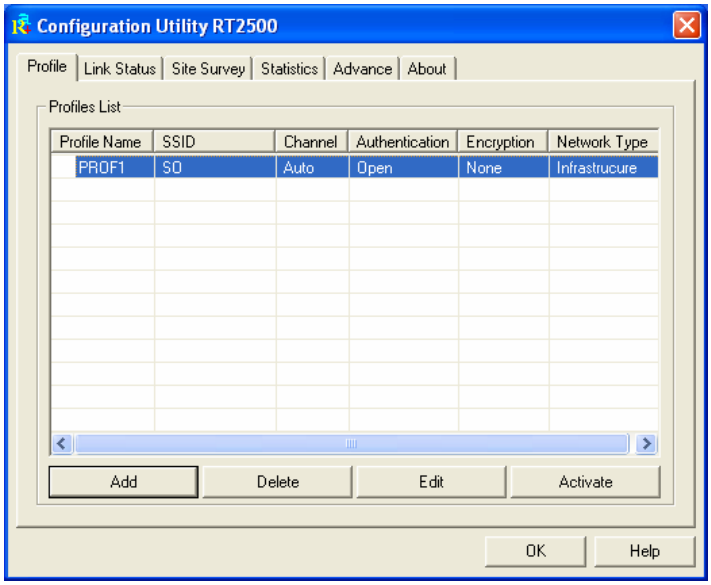
When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your card and automatically connect to the wireless device with the highest signal strength. From the “Site Survey” option, all the networks nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.



Parameter	Description
Available Networks	This list shows all available wireless networks within range of your card. It also displays the information of the networks including the SSID, BSSID, Signal Strength, Channel, Encryption, Authentication and Network Type. If you want to connect to any networks on the list, double-click the item on the list, and the card will automatically connect to the selected network.
Rescan Button	Click “Rescan” button to collect the information of all the wireless networks nearby.
Connect Button	Click “Connect” to connect to the selected network.
Add to Profile Button	Add the selected network to Profiles list.

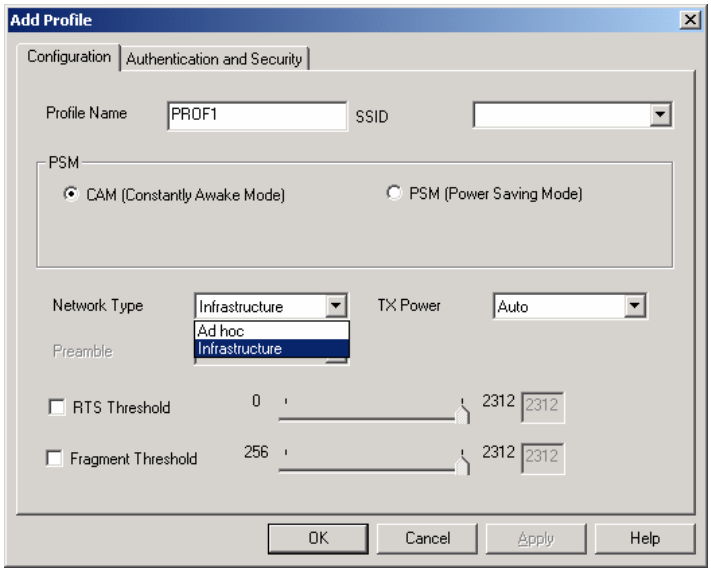
3.2 Profile

The “Profiles List” is for you to manage the networks you connect to frequently. You are able to Add/Delete/Edit/Activate a profile.



Parameter	Description
Profiles List	The profiles list display all the profiles and the relative information including Profile Name, SSID, Channel, etc.
Add/Delete/Edit Button	Click these buttons to add/delete/edit the selected profiles.
Activate Button	Click “Activate” to connect to the selected profile.

3.2.1 Configure the Profile



System Configuration

Parameter	Description
Profile Name	Define a recognizable profile name for you to identify the different networks.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the card and then only the device with the same SSID can interconnect to the card. If you want to add one of the networks nearby to the profile list, pull down the menu, all the networks nearby will be listed and you can add one of them to the profile list.
Power Saving Mode	The power saving function is only available when the network type is in Infrastructure. **CAM(Constantly Awake Mode)** – The card will always set in active mode. **Power Saving Mode** – Enable the card in the power saving mode when it is idle. **CAM When AC Power** – Select this option to automatically switch the card from power saving mode to CAM mode while the power of your laptop computer is supplied by the AC power but not battery.

Parameter	Description
Network Type	**Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad-Hoc** – Select this mode if you want to connect to another wireless stations in the Wireless LAN network without through an Access Point or Router.
Transmit Power	If you want to lower the transmit power of the card for saving the power of the system, you can select the lower percentages from the list.
11B Preamble Type	The preamble defines the length of the CRC block for communication among wireless stations. This option is only active in the Ad Hoc network. There are two modes including Auto and Long Preamble. If “Auto“ mode is selected, the card will auto switch the preamble mode depending on the wireless stations which the card is connecting to.
RTS Threshold	Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2312 bytes. Minor change is recommended.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2312 bytes. Minor change is recommended.
Channel	This setting is only available for Ad Hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same with the network you are connecting to.

Authentication vs. Security

Parameter	Description
Authentication Type	This setting has to be consistent with the wireless networks that the card intends to connect. **None** – No authentication is needed among the wireless network. **Shared** – Only wireless stations using a shared key (WEP Key identified) are allowed to connecting each other. **WPA-PSK** –It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless stations in the network. WPA takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices. The encryption methods are including TKIP and AES. Note that this option is only available for Windows XP.
802.1x Authentication 802.1x Setting	It allows to get more powerful secure when you enable it and press the 802.1x setting button, the user can establish the information that authentication is correlated with further through this picture , such as protocol , ID and password , Client evidence or server evidence of Tunnel ,etc., please refer to the following chapter 3.2.3 for detail information.
Encryption Mode	**None** – Disable the WEP Data Encryption.

	WEP – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys. **TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. Note: All devices in the network should use the same encryption method to ensure the communication.
WPA Pre-Shared Key	The WPA-PSK key can be from eight to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
WEP Key (Key1 ~ Key4)	The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Select the default encryption key from Key 1 to Key 4 by selected the radio button. Fill the text box by following the rules below. **64-bit** – Input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII characters (including “a-z” and “0-9”) as the encryption keys. For example: “0123456aef“ or “test1”. **128-bit** – Input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 13-digit ASCII characters (including “a-z” and “0-9”) as the encryption keys. For example: “01234567890123456789abcdef“ or “administrator”.

3.2.2 Enable WPA in Windows XP

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancement that strongly increases the level of data protection (encryption) and access control

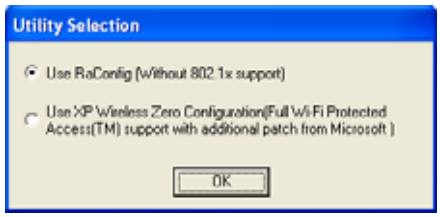
(authentication) for existing and future wireless LAN systems. The technical components of WPA include Temporal Key Integrity Protocol (TKIP) for dynamic key exchange, and 802.1x for authentication.

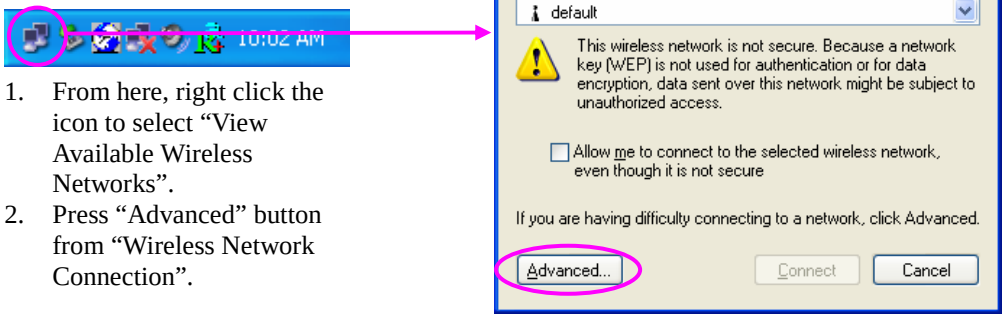
There are two types of WPA security: WPA-PSK (no server) and WPA (with server). WPA requires a Radius Server to complete the authentication among wireless stations and Access Points. Typically, this mode is used in a enterprise environment. WPA-PSK uses a so-called pre-shared key as the security key. A pre-shared key is a password that each wireless station uses the same key to access the network. Typically, this mode will be used in a home environment.

To enable the WPA function in Windows XP, the following software systems are required:

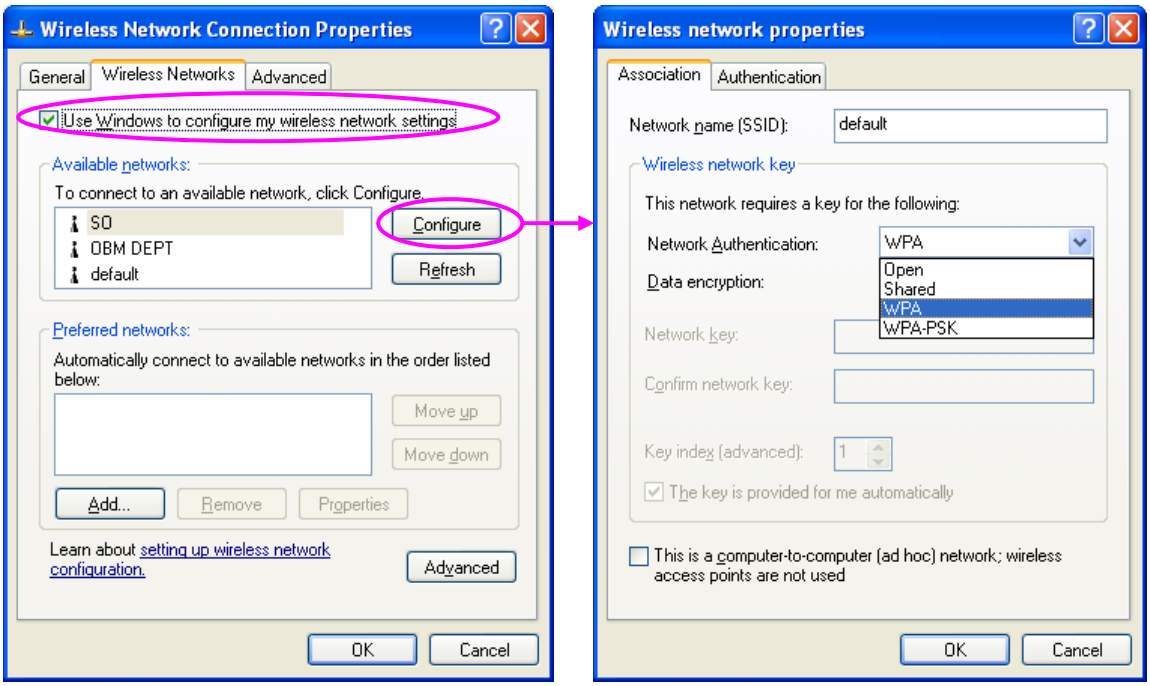
1. Windows XP Service Pack 1 with Windows XP Support Patch for Wi-Fi Protected Access program in addition.
2. Configure the card by Wireless built-in utility (Wireless Zero Configuration).

- Note: In that kind of system, there are two utility selections when you open the configuration utility of the card. You can select to use the XP's built-in utility with full WPA function. If "Use XP Wireless Zero Configuration" is selected, you can only configure the advance setting or check the link status and statistics from the "RaConfig" utility.


Utility Selection
Use RaConfig (Without 802.1x support)
Use XP Wireless Zero Configuration(Full Wi-Fi Protected Access(TM) support with additional patch from Microsoft)
OK


10:02 AM
Wireless Network Connection
The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.
Available wireless networks:
SO
OBM DEPT
default
This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.
Allow me to connect to the selected wireless network, even though it is not secure
If you are having difficulty connecting to a network, click Advanced.
Advanced...
Connect
Cancel

1. From here, right click the icon to select "View Available Wireless Networks".
2. Press "Advanced" button from "Wireless Network Connection".



3. Press “Configure” button to configure the WPA function for the current network.

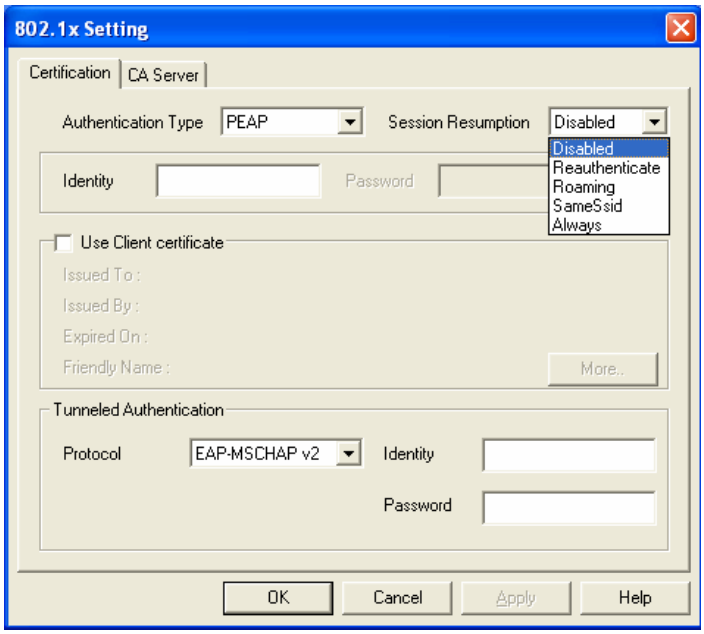
Note: Uncheck “Use Windows to Configure my wireless network settings”, the “RaConfig” utility will be enabled again.

Parameter	Description
Network Authentication	**Open** –No authentication is needed among the wireless network. **Shared** – Only wireless stations using a shared key (WEP Key identified) are allowed to connecting each other. **WPA** – This mode is for enterprise with an authentication server (Radius Server), WPA-enabled access point, and a WPA-enabled client. Once WPA is enabled, all clients and access points on the network must be WPA-enabled in order to access the network. **WPA-PSK** – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each PC on the wireless network. WPA takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

Parameter	Description
Data Encryption	**WEP** – In WPA or WPA-PSK mode, WEP is also able to be the encryption method for the transmission data. **TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. Note: All devices in the network should use the same encryption method to ensure the communication.

3.2.3 802.1x Setting _ Evidence

It will show below configuration screen when you enable the “802.1x authentication“, then press the “ 802.1x setting”.



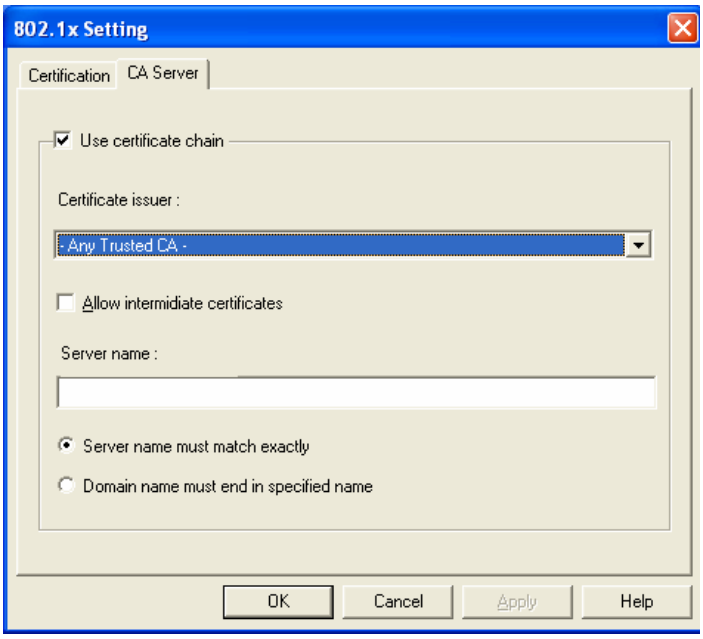
Parameter	Description
Authentication Type	There are five kinds , such as PEAP , TLS/Smartcart , TTLS , LEAP and MD5 ,etc..
Identity	User account number
Password	Password of user’s account’s number. Prove that the method is used while choosing LEAP and MD5-Challenge.
Session Resumption	We suggests to using “always” to perform the authentication with CA server.
Use Client Authenticate	Client evidence is the essential project of TLS, and the alternative projects (Option) of PEPA and TTLS. It shows that will confirm in the crossing of authentication whether Client evidence is correct to collude and select to "use Client evidence". While choosing Client evidence, press the button, will present the picture of showing the available evidence, the user can choose the suitable evidence to regard as Client evidence from it .
Tunneled Authentication	Use authentication way for two stage PEAP and TTLS when user enable each authentication method. Two stage authentication is divided into two steps, the first step is to set up Tunnel, utilized its evidence to set up one exit passageway by Server end, Station need not establish any and select, the second step is legitimacy of using the designated authentication way to confirm Station in Tunnel, the materials that authentication needs include Tunnel ID , Tunnel password , Client evidence or Server evidence.
Protocol	Authentication way to use in the exit passageway.
Identity	User's name.
Password	Password

3.2.4 802.1x Setting _ CA Server

CA server uses while adopting authentication ways, such as TLS, TTLS and PEAP, etc. Client can prove first whether this server is a dependable server, after proving that passes, convey the evidence (if enables to select to "use Client evidence").

Prove that CA server is divided into two steps:

1. Confirm whether the server evidence (Server Certificate) is authorized the unit to send out by the designated evidence, if " proving while allowing " is hit and colluded , show that this server evidence can authorize the unit (that a dependable evidence authorize the unit approved of the unit) to send out from a relaying evidence .
2. Check whether the server name of the server evidence accords with user's name input or belongs to the same network.

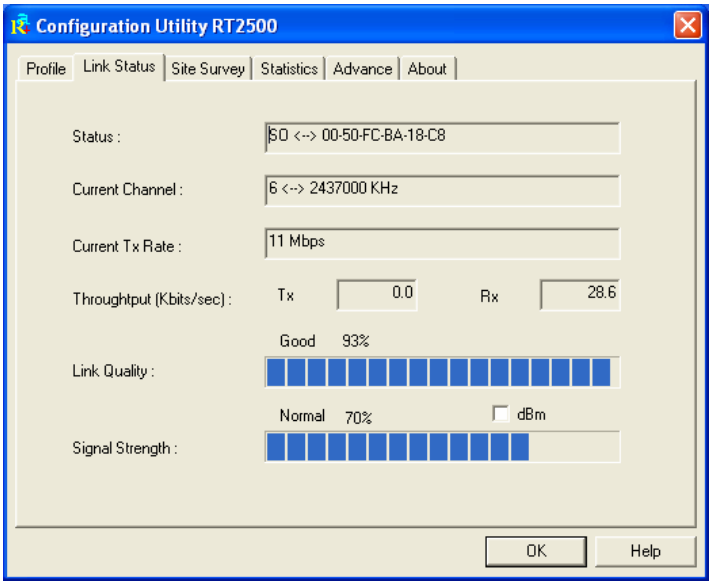


Parameter	Description
Use Certification chain	It shows that in the passing of authentication, Client will go to confirm whether CA server is a dependable server to collude and select this to select.
Certification issuer	Refer to CA of the server evidence (Server Certificate), can select to choose the suitable evidence to authorize the unit in the form from making the drawing type .
Allow intermidiate certificates	If this selects and hits colluding , show and issue (issue) The unit of the server evidence can be a evidence chosen by user to authorize the evidence approved of the unit to authorize the unit (authorize the unit or the secondary evidence to authorize the unit by relaying evidence). On the contrary, the server evidence must be that the evidence chosen by user authorize the unit to issue.
Server name	This field is made according to selecting (checkbox), its value can be the server name or the domain name of the server.

- The server name must be totally correct: If choose this to select, the server name which shows the server evidence must be self-same as "server name ".
- The server name only needs the last domain name to be the same: If choose this to select , show that the evidence which issues the server evidence authorizes the unit to be the network land or network land once input in "server name".

3.3 Link Status

From the “Link Status” option, you can view all the information of the network you are connecting to.

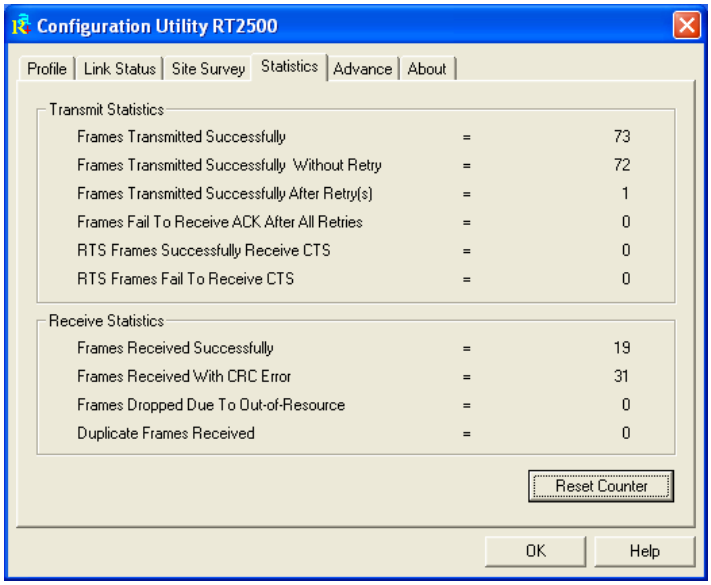


Parameter	Description
Status	Display the SSID and MAC ID of the network the card is connecting to.
Current Channel	Display the number of the radio channel and the frequency used for the networking.
Current Tx Rate	Display the transmission rate of the network. The maximum transmission rate is 54Mbps.
Throughput (Kbits/sec)	Display the speed of data transmitted and received.
Link Quality	This bar indicates the quality of the link. The higher the

	percentage, the better the quality.
dBm	If you want to know the signal strength in the unit of dBm, select this check box.
Signal Strength	This bar shows the signal strength level. The higher percentage shown in the bar, the more radio signal been received by the card. This indicator helps to find the proper position of the wireless device for quality network operation.

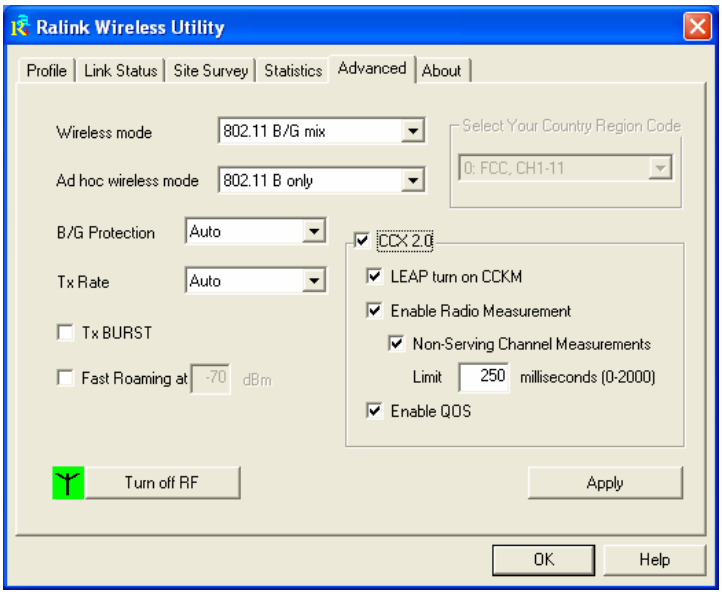
3.4 Statistics

This option enables you to view the available statistic information with its Tx counts (Tx success, Tx error, RTS Success and RTS Failed), and its Rx counts (Rx success, Rx error). You may reset the counters by clicking ”Reset Counter”.


Configuration Utility RT2500
Profile
Link Status
Site Survey
Statistics
Advance
About
Transmit Statistics
Frames Transmitted Successfully = 73
Frames Transmitted Successfully Without Retry = 72
Frames Transmitted Successfully After Retry(s) = 1
Frames Fail To Receive ACK After All Retries = 0
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Receive Statistics
Frames Received Successfully = 19
Frames Received With CRC Error = 31
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
Reset Counter
OK
Help

3.5 Advance

This option enables you to configure more advanced settings, for example: wireless mode, protection mode and etc.

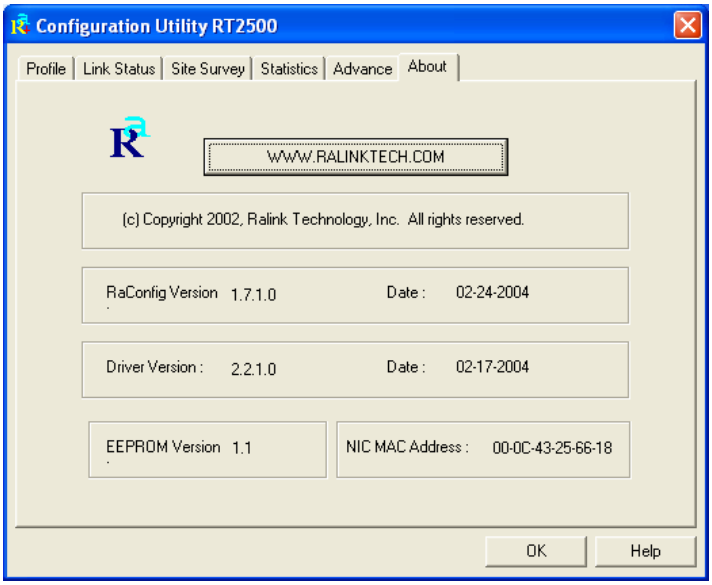


Parameter	Description
Wireless Mode	**802.11 B/G mix** – If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended to setting the card to this mode. This mode is also the default setting. **802.11 B only** – This card can be compatible with both 802.11g and 802.11b wireless stations. If there are only 802.11b wireless stations in the network, you can set the card to this mode.
AD hoc wireless mode	When the network type is in Ad Hoc mode that the card can only work in 11b data rate. It is defined by Wi-Fi organization. If you want to enable the data rate up to 54Mbps (11g), select “Adhoc wireless mode”.
B/G Protection	If you have a mix of 802.11b and 802.11g wireless stations in the network, it is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the card will be a little lower due to many of frame traffic should be transmitted. **Auto** – Based on the status of the network and automatically disable/enable protection mode. **On** – Always enable the protection mode. **Off** – Always disable the protection mode.
Tx Rate	There are several options including Auto/1/2/5.5/11/6/9/12/18/24/36/48/54Mbps for you to select. When the “Auto” is selected, the device will choose the most

	suitable transmission rate automatically. The higher data rate you designated in the network, the shorter distance is allowed between the card and the wireless stations. When the wireless mode is “802.11 B only”, the maximum data rate is 11Mbps (11b) so that there are only “Auto/1/2/5.5/11Mbps” options you can select.
Tx BURST	Tx Burst enables the card to deliver the better throughput in the same period and environment.
Fast Roaming at	Unless under at situation that roam, if there are two Cisco’s AP in environment, and not as performance that link of now in lower than - 70dbm at, it will switch over it to another one AP automatically.
Select your country region code	It allows to change the domain from CCS tool, you can enable this feature from Program/RaLink/RT2500/CCS
CCX 2.0	When you enable this feature and it allows to perform the relating functions with Cisco wireless device.

3.6 About

By choosing this option, you can click the hyperlink to connect the website for the information of the wireless chipset vendor and review basic information about the Utility such as the Driver, Utility and EEPROM Version. The MAC Address of the card is displayed in the screen as well.



4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard？

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. What does IEEE 802.11 feature support？

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. What is Ad-hoc？

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure？

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID？

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP？

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing？

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air？

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS？What is FHSS？And what are their differences？

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).